

IPv6: Privacy Extensions einschalten


Automatische IPv6-Konfiguration mit Tarnkappe

Reiko Kaps - 13.04.11


Die automatische IPv6-Einrichtung (Stateless Address Autoconfiguration, SLAAC) nutzt auf einigen Betriebssystemen per Vorgabe die Hardware-Adresse der Netzwerkschnittstelle. Solche Adressen sind im Internet leicht wiederzuerkennen. Abhilfe schaffen die Privacy Extensions, die zusätzliche, über Zufallszahlen generierte und wechselnde IPv6-Adressen erzeugen.

Das Internet Protocol Version 6 (IPv6) hat bereits einige Jahre auf dem Buckel, trotzdem schleppt es auf manchen Betriebssystemen noch Probleme aus seiner Anfangszeit mit. Dazu gehört etwa, dass Rechner für die automatische Adresseinrichtung via Router Advertisement die eindeutige Hardware-Adresse (MAC) der jeweiligen Netzwerkkarte nutzen können. Das Stateless Address Autoconfiguration genannte Verfahren schiebt in der Mitte der nur 48 Bit langen MAC-Adresse zusätzlich die Bytes `ff:fe` ein und erzeugt daraus den Local Identifier, also die hinteren 64 Bit einer IPv6-Adresse. Die ersten 64 Bit gehören dem Netzwerk-Präfix, das der IPv6-Router im Netzwerk bekannt gibt und das der Rechner in die globale IPv6-Adresse übernimmt.



Ohne Eingriff leiten Linuxe und Mac-OS-Rechner ihre globale IPv6-Adresse aus der Hardware ab - und offenbaren damit viel über den Benutzer.  Selbst den IPv6-Entwicklern fiel schnell auf, dass dieses Verfahren die Privatsphäre von Rechner und Nutzer gefährdet. Solche statischen IPv6-Adressen wirken wie eine eindeutige Hardware-ID, die der Rechner bei jedem Kontakt zu einem IPv6-tauglichen Server überträgt. Brisant ist das bei Geräten wie Tablets oder Smartphones, denn sie werden in der Regel nur von einer Person genutzt. Die für jeden Serverbetreiber und Netzbeobachter zugängliche MAC-Adresse erlaubt es damit, diese Person wiederzuerkennen.



Windows (seit Vista) erzeugt immer eine temporäre IPv6-Adresse, die dem Nutzer mehr Privatheit verschafft.  Daher definierten sie nachträglich das Verfahren "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" ([RFC 4941](http://tools.ietf.org/html/rfc4941)), mit dem sich zusätzlich zu diesen

statischen Adressen temporäre erzeugen lassen, die der Rechner für seine Anfragen ins IPv6-Internet einsetzt. Der Host Identifier dieser Adressen wird über Zufallszahlen ermittelt.

Allerdings setzen längst nicht alle aktuellen Betriebssysteme diese Erweiterung ab Werk ein. Derzeit hat einzig Windows die Privacy Extensions eingeschaltet. Andere wie Mac OS und Linux beherrschen das Verfahren zwar, man muss es aber per Hand aktivieren. Der folgende Artikel erklärt, wo man auf den unterschiedlichen Systemen die nötigen Schalter findet.

Betriebssystem	Privacy Extensions	ab Werk aktiv	de-/aktivierbar	Anmerkung
Windows XP	+	+	+/+	
Windows Vista	+	+	+/+	
Windows 7	+	+	+/+	
Windows Server 2003	+	-	+/+	
Windows Server 2008 R2	+	-	+/+	
OpenSuse Linux	+	-	+/+	
Ubuntu Linux	+	ab 12.04	+/+	
Debian Linux	+	-	+/+	
Fedora Linux	+	-	+/+	
Mac OS X	+	ab 10.7	+/+	
iOS 4.1	+	-	-/-	Privacy Extensions via Jailbreak
iOS 4.2	+	-	-/-	Privacy Extensions via Jailbreak
iOS 4.3	+	+	-/-	
Android ab 2.1	+	-	-/-	Privacy Extensions über Rooting

Windows XP, Vista und 7

Ohne dass der Nutzer eingreifen muss, richten die Desktop-Versionen von Windows per Stateless Autoconfiguration bereits temporäre IPv6-Adressen ein. Wie im RFC vorgesehen wechselt Windows diese Adressen in Intervallen, die sich wie auch andere IPv6-Parameter über das Kommando `netsh` einstellen lassen. Da wechselnde Adressen auf Servern eher

weniger sinnvoll sind, hat Microsoft die Privacy Extensions auf seinen Windows-Server-Versionen nicht ab Werk eingeschaltet.

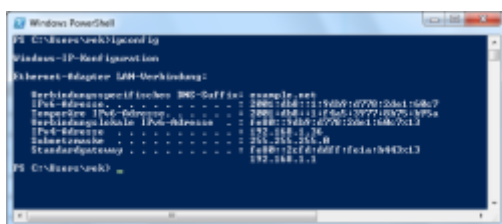
Anders als andere erzeugen Windows-Rechner ihre statische IPv6-Adresse auch nicht aus der Hardware-Adresse der jeweiligen Schnittstelle. Stattdessen würfelt Windows die Adresse einmal, meist bei der Installation, aus. Dieses voreingestellte Verhalten lässt sich als Administrator jedoch ändern. Mit dem Befehl

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```

nutzt Windows für seine statische, globale IPv6-Adresse nun die MAC der Netzwerkschnittstelle. Die aktuelle Einstellung für diese Vorgabe zeigt das Kommando `netsh interface ipv6 show global` in der Ausgabezeile "IDs zufällig anordnen" an.

Die aktuellen IPv6-Adressen aller Netzwerkkarten zeigt der Befehl `netsh interface ipv6 show addresses`, mit `netsh interface ipv6 show privacy` gibt Windows die Vorgaben für die Privacy Extensions aus:

```
C:\>netsh interface ipv6 show privacy
Der aktive Status wird abgefragt...
Parameter für temporäre Adressen
-----
Temporäre Adresse verwenden           : enabled
Versuch, doppelte Adr. zu entdecken  : 5
Maximale Gültigkeitsdauer             : 7d
Maximale bevorzugte Gültigkeitsdauer : 1d
Regenerationszeit                    : 5s
Maximale Verzögerungszeit             : 10m
Verzögerungszeit                     : 0s
```



Windows erzeugt seine feste IPv6-Adresse nicht über die MAC, die Privacy Extensions hat Microsoft ab Werk aktiviert. Die Ausgabe bestätigt, dass die Privacy Extensions (Temporäre Adresse verwenden) aktiv sind. Der Wert hinter "Maximale bevorzugte Gültigkeitsdauer" legt fest, nach welcher Zeit (hier in Tagen) der Rechner eine neue temporäre Adresse erzeugt und für ausgehende Pakete auch einsetzt. Eingehende Verbindungen akzeptiert der Rechner deutlich länger (Maximale Gültigkeitsdauer) auf einer temporären Adresse, was etwa für Peer-to-Peer-Anwendungen nützlich sein kann.

Will man die temporären IPv6-Adressen vollständig abschalten, reicht der Befehl

```
netsh interface ipv6 set privacy state=disabled
```

Die Werte für "Maximale bevorzugte Gültigkeitsdauer" und "Maximale Gültigkeitsdauer" setzt man über die Schlüssel `maxpreferredlifetime` und `maxvalidlifetime`, die Zeitangaben in Tagen (d), Stunden (h), Minuten (m) und Sekunden (s) entgegennehmen:

```
netsh interface ipv6 set privacy maxpreferredlifetime=12h
```

Dieses Kommando halbiert die Lebensdauer einer temporären IPv6-Adresse auf 12 Stunden. Mit `netsh interface ipv6 set privacy maxvalidlifetime=2d` verringert man die Zeitspanne, in der Windows über eine temporäre IPv6-Adresse eingehende Pakete empfängt.

Linux: Debian/Ubuntu, Fedora

Alle großen Linux-Distributionen schalten IPv6 ein, die Privacy Extensions aktivieren sie jedoch nicht. Das bemerkt man schnell an den aus der Hardware-Adresse abgeleiteten Adressen, die im hinteren Teil die Bytes `ff` und `fe` enthalten.

Die Privacy Extensions lassen sich über das Sysctl-System dauerhaft einschalten. Am einfachsten gelingt das, wenn man für jede Netzwerkschnittstelle im Computer die Zeile

```
net.ipv6.conf.IF.use_tempaddr = 2
```

in die Datei `/etc/sysctl.conf` nachträgt. Den Platzhalter `IF` müssen Sie dabei durch die Schnittstellenbezeichnung ersetzen, also etwa `eth0` für die erste Ethernet-Karte oder `wlan0` für das WLAN-Interface. Testweise können Sie den Sysctl-Wert auch direkt über die Shell eingeben:

```
sudo sysctl net.ipv6.conf.wlan0.use_tempaddr=2
```

Damit Linux die Netzwerkschnittstelle mit einer temporären IPv6-Adresse versorgt, müssen Sie die Schnittstelle einmal aus- und wieder einschalten (etwa über den Network Manager). Anschließend zeigt `ifconfig` an der Schnittstelle eine weitere IPv6-Adresse, deren hinterer Teil nicht mehr aus der Hardware-Adresse abgeleitet wurde. Dass es sich tatsächlich um eine temporäre Adresse handelt, zeigt der Befehl `ip -6 addr show` über den Bezeichner "temporary" in seinen Ausgaben an.

Während diese Befehle unter OpenSuse und Fedora für das Aktivieren der Privacy Extensions ausreichen, muss man unter Ubuntu zusätzlich den Wert `net.ipv6.conf.default.use_tempaddr=2` in der Datei `/etc/sysctl.conf` setzen.

Opensuse

Opensuse kennt zwar eine Systemvariable `IPV6_PRIVACY`, die Sie mit dem Sysconfig-Editor in Yast auf "Yes" setzen können. Doch führte das in unseren Versuchen auch mit weiteren Anpassungen an Systemskripten nicht zum Erfolg – nutzen Sie stattdessen den oben beschriebenen Weg über `/etc/sysctl.conf`.

Auch die Vorgaben zum Wechseln der temporären IPv6-Adresse lassen sich via `sysctl` anpassen: Die Sysctl-

Schlüssel `net.ipv6.conf.IF.temp_valid_lft` und `net.ipv6.conf.IF.temp_prefered_lft` setzen die maximale Zeit in Sekunden, in der Linux die Adresse für eingehende und ausgehende Anfragen nutzt. Der letzte Schlüssel hat typischerweise den Wert 86400 (24 Stunden), eingehende Pakete akzeptiert Linux sieben Tage an dieser Adresse. Den Platzhalter IF müssen Sie dabei wie oben durch den Schnittstellennamen ersetzen.

Android

Googles Smartphone-Betriebssystem setzt auf Linux auf, das zufällige und wechselnde IPv6-Adressen erzeugen kann. Andererseits hat Google die dafür nötigen Vorgaben nicht gesetzt, sodass bislang jede Android-Version ohne die Privatsphäre schützenden IPv6-Adressen auskommen muss. Auch lassen sie sich nicht einfach einschalten, denn die Mobilfunk-Provider und Handy-Hersteller vernageln den dafür nötigen Root-Zugang.



Zwei Befehle genügen und ein gerootetes Android surft über die wechselnden und nicht aus der Hardware abgeleiteten IPv6-Adressen. ☹ Wie auch auf iPhones bleibt nur der Weg über das nachträgliche Freischalten des Root-Zugangs oder über die Installation von Custom-ROMs: Mit dem für solche Verwaltungsaufgaben nötigen Root-Benutzer lassen sich dann wieder die Sysctl-Werte setzen, die die Privacy Extensions für IPv6 aktivieren. Steht auf dem Telefon das Kommando `su` bereit, reichen die Befehle

```
su
sysctl -w net.ipv6.conf.default.use_tempaddr=2
sysctl -w net.ipv6.conf.all.use_tempaddr=2
```

Nach einem Neustart vergisst Android diese Einstellungen jedoch wieder. Man kann die beiden Befehle allerdings in eine Datei namens `/data/local/userinit.sh` schreiben. Existiert diese Datei, führt Cyanogenmod die darin aufgelisteten Befehle beim Systemstart aus.

Mac OS X

Wie Linux kann auch Apples Betriebssystem Mac OS X über die Privacy Extensions ermittelte IPv6-Adressen erzeugen und einsetzen. Allerdings hat Apple dafür keinen Schalter vorgesehen. Das Programm **IPv6 Anonymizer** von c't zeigt den Status der Privacy Extensions, schaltet sie an oder aus und sorgt dafür, dass die Funktion auch beim Neustart zur Verfügung steht. IPv6 Anonymizer steht im Heise Softwareverzeichnis zum [Download](#) bereit.



Das Mac-Programm IPv6 Anonymizer zeigt und setzt die Einstellungen für die Privacy Extensions per Maus-Klick. Wer lieber selbst Hand anlegt, kann auch die Kommandozeile benutzen. Die Privacy Extensions lassen sich im Terminal (im Dienstprogramme-Ordner) mit dem Befehl

```
sudo sysctl -w net.inet6.ip6.use_tempaddr=1
```

aktivieren. Das vorangestellte `sudo` fragt nach Ihrem Passwort und führt dann den Befehl `sysctl` mit Administrator-Rechten aus. Damit das klappt, müssen Sie mit einem Benutzer angemeldet sein, der den Mac verwalten darf. Leider verschwindet die Einstellung nach einem Neustart.

iPhone und iPad (iOS)

Noch schlechter als auf dem Apple-Desktop sah es bis vor kurzem unter den Mobil-Betriebssystemen für iPhones und iPads aus. Bis zur Version 4.3 waren auch dort die Privacy Extensions abgeschaltet. Erst das Update aktiviert die Erweiterung. Im Unterschied zu Mac OS X steht aber auf den Mobilbetriebssystemen für iPhone und iPad kein vom Hersteller vorgesehener Weg offen, die Privacy Extensions zu aktivieren oder abzuschalten.

Will man auf Geräten mit der IOS-Version kleiner als 4.3 die Privacy Extensions einschalten, hat man nur dann eine Chance, wenn man einen Administrator-Zugang zum Betriebssystem hat (Jailbreak): In diesem Fall reicht der Aufruf von

```
sudo sysctl -w net.inet6.ip6.use_tempaddr=1
```

respektive der Eintrag

```
net.inet6.ip6.use_tempaddr=1
```

in die Datei `/etc/sysctl.conf`. Starten Sie dazu im Terminal einen Editor mit root-Rechten, beispielsweise mit

```
sudo pico /etc/sysctl.conf
```

und fügen Sie die Zeile am Ende der Datei an. Nach einem Neustart der WLAN-Schnittstelle respektive einem Neustart des Geräts sollte die Webseite <http://ct.de/ip> die zweite, über die Privacy Extensions erzeugte IPv6-Adresse anzeigen.